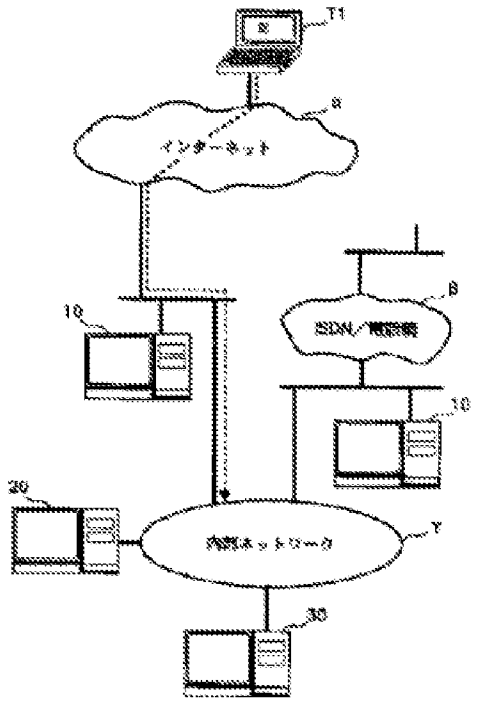
METHOD AND SYSTEM FOR DECIDING ACCESS TYPE IN COMMUNICATION NETWORK AND RECORDING MEDIUM

Publication number: JP2001313640
Publication date: 2001-11-09
Inventor: BABA TATSUYA; YAMAOKA MASATERU; KOKUBO KATSUTOSHI; MATSUDA YOSHIYUKI
Applicant: NTT DATA CORP
Classification:
- international: ***G06F13/00; H04L12/22; H04L12/24; H04L12/26;*** **G06F13/00**; **H04L12/22**; **H04L12/24**; **H04L12/26**; (IPC1-7): H04L12/24; G06F13/00; H04L12/22; H04L12/26
- European:
Application number: JP20000133494 20000502
Priority number(s): JP20000133494 20000502

Report a data error here

Abstract of **JP2001313640**

PROBLEM TO BE SOLVED: To provide an illegal access detection system capable of detecting illegal accesses of various patterns including an unknown method. SOLUTION: The latest access policy of a site to be a management object is acquired from a management server 20 and held. Packets addressed to the site are acquired among packets circulated in a network, and packets suitable for the access policy and packets unsuitable for the access policy are sorted amount the acquired packets. When a packet unsuitable for the policy is selected, the packet is specified as a packet having possibility of being an illegal access and notified to the management server 20 in order to change an access condition for removing an access based on the specified packet.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－313640
（P2001－313640A）
(43)公開日　平成13年11月９日(2001.11.9)

(51)Int.Cl.[7]		識別記号	FI			テーマコード（参考）
Ｈ０４Ｌ	12/24		Ｇ０６Ｆ	13/00	３５１Ｚ	５Ｂ０８９
	12/26		Ｈ０４Ｌ	11/08		５Ｋ０３０
Ｇ０６Ｆ	13/00	３５１		11/26		９Ａ００１
Ｈ０４Ｌ	12/22					

審査請求　未請求　請求項の数５　ＯＬ　（全 11 頁）

(21)出願番号　特願2000－133494(P2000－133494)

(22)出願日　平成12年５月２日(2000.5.2)

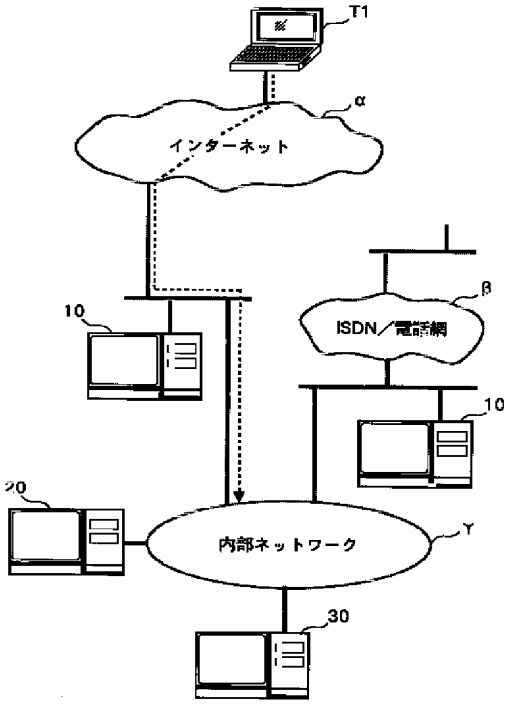
特許法第30条第１項適用申請有り　平成12年３月14日～３月16日　社団法人情報処理学会主催の「第60回（平成12年前期）全国大会」において文書をもって発表

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　馬場　達也
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　山岡　正輝
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100099324
弁理士　鈴木　正剛

最終頁に続く

(54)【発明の名称】　通信ネットワークにおけるアクセス種別を判定する方法及びシステム、記録媒体

(57)【要約】
【課題】　未知の手法を含む種々のパターンの不正アクセスを検知可能な不正アクセス検知システムを提供する。
【解決手段】　管理対象となるサイトの最新のアクセスポリシーを管理サーバ２０から取得して保持しておく。ネットワークを流通するパケットの中からサイト宛のものを捕獲し、捕獲したパケットの中からアクセスポリシーに適合するパケットと適合しないパケットとを選別する。適合しないパケットが選別されたときは、これを不正アクセスの蓋然性があるパケットとして特定し、その特定したパケットに基づくアクセスを排除するためのアクセス条件の変更等を行わせるために、管理サーバ２０に通知する。



【特許請求の範囲】
【請求項１】　通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するためのプロトコル仕様及び／又はアクセスポリシーを、対象となる通信システム又は通信システムグループ毎に定めておき、前記通信ネットワークを流通する伝送情報の中から前記通信システム又は通信システムグループ宛の伝送情報を捕獲するとともに、捕獲した伝送情報の中から前記プロトコル仕様及び／又はアクセスポリシーに適合しない伝送情報を不正アクセスの蓋然性がある伝送情報として特定する過程を含む、
通信ネットワークにおけるアクセス種別を判定する方法。
【請求項２】　通信ネットワークに存在する通信システム又は通信システムグループのアクセス管理を行う管理サーバと、この管理サーバによるアクセス管理の補助処理を行う不正アクセス検知システムとを含み、
前記管理サーバは、
前記通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録する条件情報登録手段と、
各通信システム又は通信システムグループに対するアクセス許可条件の変更を行う条件変更手段とを有するものであり、
前記不正アクセス検知システムは、
前記管理サーバの条件情報登録手段から最新の前記条件情報を取得する条件情報取得手段と、
前記通信ネットワークを流通する伝送情報の中から管理対象となる通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段と、
捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段と、
前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す通知手段とを具備するものである、
通信ネットワークにおけるアクセス種別を判定するシステム。
【請求項３】　通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を対象となる通信システム又は通信システムグループ毎に更新自在に保持する条件情報保持手段と、
前記通信ネットワークを流通する伝送情報の中から前記通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段と、
捕獲した伝送情報の中から最新の前記条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段とを具備し、
前記第２伝送情報を不正アクセスの蓋然性がある伝送情報として扱うことを特徴とする、不正アクセス検知システム。
【請求項４】　外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録してなる条件情報登録手段と、各通信システム又は通信システムグループに対するアクセス条件の変更を行う条件変更手段とを有する通信ネットワークに接続され、
前記条件情報登録手段から最新の前記条件情報を取得する条件情報取得手段と、
前記通信ネットワークを流通する伝送情報の中から前記取得した条件情報に対応する通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段と、
捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段と、
前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す通知手段とを具備し、
前記第２伝送情報を不正アクセスの蓋然性がある伝送情報として扱うことを特徴とする、不正アクセス検知システム。
【請求項５】　外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録してなる条件情報登録手段と、各通信システム又は通信システムグループに対するアクセス条件の変更を行う条件変更手段とを有する通信ネットワークに接続される通信機能付きコンピュータに、
前記条件情報登録手段から最新の前記条件情報を取得する処理と、
前記通信ネットワークを流通する伝送情報の中から前記取得した条件情報に対応する通信システム又は通信システムグループ宛の伝送情報を捕獲する処理と、捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する処理と、
前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す処理とを実行させるためのプログラムコードが記録された、
コンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】

【発明の属する技術分野】本発明は、イーサネット（登録商標）やインターネットのような通信ネットワークにおいて発生する不正アクセスを検知する手法に係り、より詳しくはアクセス先に於いて固有となる正常アクセスの条件を定めた条件情報をもとに、未知のパターンの不正アクセスも検知することができるようにする方法及びそれを実現するためのシステム技術に関する。

【０００２】

【従来の技術】多数の者がアクセス可能な通信ネットワークに接続されている通信システム又は内部ネットワーク等によって構築される通信システムグループ（以下、便宜上、これらを総称して「サイト」と称する）に対して当該通信ネットワーク経由で不正に行われるアクセス（以下、「不正アクセス」）を検知する手法として、従来、以下の３つの方式が知られている。

【０００３】第１の方式は、既存の不正アクセスの特徴パターン（以下、「シグネチャ」と称する。）、例えば、通信プロトコルの種類、パケットの大きさ、そのパケットのデータ部に含まれている文字列等の組み合わせを予め検知対象となる不正アクセスの数だけ保持しておき、所定の検知システムが、ネットワーク上を流れるパケットを捕獲してアクセス内容を監視し、そのアクセスの内容がシグネチャと一致した場合に、不正アクセスが発生したとして、そのアクセスの内容と発信源の情報とを管理者等に知らせる方式である。この方式を採用する既存のソフトウエアとしては、アメリカ合衆国Cisco Systems, Inc社の「Cisco Secure IntrusionDetection System」（同社の商標），アメリカ合衆国Internet Security Systems, Inc社の「RealSecure」（同社の商標）等がある。

【０００４】第２の方式は、通信ネットワークのユーザ毎のアクションパターンデータを使用するもので、その詳細は、下記文献に示されている。

（１）H.S.Javits and A.Valdes.The SRI IDES Statistical Anomaly Detector.In Proceedings of the IEEE Symposium on Security and Privacy,May 1991

（２）岡本他，なりすましに対する不正侵入検知システム（IDS－M），信学技報OFS99－15，AI99－27，pp. 39－46，July 1999

この方式は、要するに、ログインしているユーザ毎に、所定の検知システムが、対象システム内でのアクションパターンデータ、例えばコマンドの種類、順序、使い方等の統計データを長期的に収集することで、平均的な通常アクセスのパターン、すなわち、プロファイルをその統計から生成し、そのプロファイルから大きく離れた行動をした場合に、正規ユーザになりすました不正アクセスが発生したとして警告を発する方式である。

【０００５】第３の方式は、利用サービスやアクセス先機器毎のアクセスパターンデータを使用するもので、その詳細は、下記文献に示されている。

（３）P.A Porras and P.G Neumann. EMERALD:Event monitoring enabling responses to anomalous live disturbances. In Proceeding of the 20th NationalInformation Systems Security Conference. pp.353-365.Oct. 1997

この方式では、所定の検知システムが、利用プロトコルやアクセス先アドレス毎にアクセスの内容、手順等の統計を長期的に収集することで、第２方式と同様、プロファイル（但し、この場合のプロファイルは、アクセスパターンデータとなる）を生成する。そして、生成したプロファイルから大きく離れたアクセスが発生した場合に不正アクセスが発生したとして警告を発する。

【０００６】

【発明が解決しようとしている課題】しかしながら、従来の各方式には、以下のような問題点があった。第１の方式では、予め登録されているシグネチャに対応する不正アクセスのみが検知対象であるため、未知の手法の不正アクセスを検知することができない。また、新しい手法のシグネチャの作成と登録までの間に、その新しい手法による不正アクセスが自由に行われる可能性が高く、不正アクセスを行う者（「攻撃者」）が攻撃対象のシステムの管理者に気づかれずに行われる不正アクセスの範囲が広がる可能性がある。

【０００７】第２及び第３の方式では、攻撃者が、検知システムに警告されない程度に通常アクセスパターンから少し逸脱したアクセスを継続して行っていくことで、検知システムの統計を狂わせ、その結果、検知システムにおいて異常であると判断するための基準を攻撃者の都合の良いようにずらしていくことが可能である。つまり、攻撃者は、最終的に自分が行おうとする不正アクセスを検知システムの通常アクセスの範囲内に収めてしまうことが可能となる。そうすると、検知システムは、もはやそのアクセスを不正アクセスであると判断することができなくなる。また、通常アクセスパターンからどの程度逸脱したら不正アクセスとして検知するのか、その判断の基準が非常に曖昧となり、検知結果に確信が持てなくなる。さらに、不特定多数のユーザの利用を許可するようなサービス、例えばインターネットにおけるWWW（world wide web）、電子メール、DNS（domain name service）等の場合には、ユーザ毎のプロファイルは作成できないし、実際のアクセスの統計を長時間取らなければならないため、導入後すぐに利用することが困難である。

【０００８】本発明は、上記の問題点に鑑み、未知の手法を含めた広範囲のアクセス種別を判定することができ、且つ判定の基準を攻撃者に操作されることがない新たな仕組みを提供することを主たる課題とする。

【０００９】

【課題を解決するための手段】上記の課題を解決するため、本発明では、上記のシグネチャを登録しておくとい

う既存の不正アクセス検知方法では、未知の手法に対応できないことや頻繁なアップデートの必要性があることから、逆に、シグネチャではなく、正常アクセスのための条件に適合するかどうかで不正アクセスの蓋然性の有無を判定する新たな手法を採用する。ここでいう「正常アクセス」とは、実際のアクセスの統計から得られる通常のアクセスとは類似するものの、本質的な相違がある。通常のアクセスには正常アクセスに加えて、怪しいアクセスも含まれる。これに対して、正常アクセスは、実際のアクセスからではなく、予め定められたアクセス条件に基づくものであって、運用時にそれが変更されることはない。そのアクセス条件が変更されるのは、通信ネットワークの構成が変更された場合のみである。このため、上記の従来技術のように、運用中に攻撃者に変更されるおそれもない。「正常なアクセスのための条件」は、例えば、（１）アクセスに使用されるプロトコルの仕様に準拠しているかどうか、（２）管理対象となる通信システム又は通信システムグループのアクセスポリシー（例えばあるホストを保持する組織がそのホストに対して許可したアクセス条件を定めた情報。実際にはアクセスを制限するための条件が記述される。送信元アドレス／宛先アドレス／利用プロトコル（ポート番号）／これら組合せは、その一例となる）に準拠しているかどうか、（３）プロトコルポリシー（プロトコルで使用されているコマンドやＵＲＬ等の内容、データの長さ）に準拠しているかどうか、（４）単位時間あたりのアクセスの回数が、上記のアクセスポリシーに記述されているアクセスの許容頻度以内であるかどうか、という観点から決定する。その後、各チェックの結果を予め学習されたニューラルネットワークに入力し、危険度を定量化する。この危険度が一定値以上であれば、発信源の追跡手段で追跡を行うことになる。この追跡手段については、例えば本願出願人による特開２０００－１２４９５２号公報に記載された技術を用いることができる。なお、（２）における「通信システムグループ」とは、ＬＡＮ等の内部ネットワークによってグループ化された通信システムをいう。

【００１０】上記の思想を具現化した本発明の方法は、通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するためのプロトコル仕様及び／又はアクセスポリシーを、対象となる通信システム又は通信システムグループ毎に定めておき、前記通信ネットワークを流通する伝送情報の中から前記通信システム又は通信システムグループ宛の伝送情報を捕獲するとともに、捕獲した伝送情報の中から前記プロトコル仕様及び／又はアクセスポリシーに適合しない伝送情報を不正アクセスの蓋然性がある伝送情報として特定する過程を含む、通信ネットワークにおけるアクセス種別を判定する方法である。

【００１１】本発明は、また、上記アクセス種別を判定する方法の実施に適したシステムを提供する。　このシステムは、通信ネットワークに存在する通信システム又は通信システムグループのアクセス管理を行う管理サーバ（２０）と、この管理サーバ（２０）によるアクセス管理の補助処理を行う不正アクセス検知システム（１０）とを含んで構成される。便宜上、後述する実施の形態に対応する参照符号を付して、その構成を具体的に説明する。管理サーバ（２０）は、前記通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録する条件情報登録手段２１，ＤＢ２２）と、各通信システム又は通信システムグループに対するアクセス許可条件の変更を行う条件変更手段（２２，ＤＢ２３）とを有するものである。また、不正アクセス検知システム（１０）は、前記管理サーバの条件情報登録手段から最新の前記条件情報を取得する条件情報取得手段（１１）と、前記通信ネットワークを流通する伝送情報の中から管理対象となる通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段（１２）と、捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段（１３，１４，１５）と、前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す通知手段（１６）とを具備するものである。

【００１２】上記の不正アクセス検知システム（１０）は、以下のような構成も可能である。すなわち、通信ネットワークを介して外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を対象となる通信システム又は通信システムグループ毎に更新自在に保持する条件情報保持手段（ＤＢ１１，ＤＢ１２）と、前記通信ネットワークを流通する伝送情報の中から管理対象となる通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段（１２）と、捕獲した伝送情報の中から最新の前記条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段（１３，１４，１５）とを具備し、第２伝送情報を不正アクセスの蓋然性がある伝送情報として扱う構成。

【００１３】外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録してなる条件情報登録手段（２１，ＤＢ２２）と、各通信システム又は通信システムグループに対するアクセス条件の変更を行う条件変更手段（２２，ＤＢ２３）とを有する通信ネットワークに接続され、前記条件情報登録手段から最新の前記条件情報を取得する条件情報取得手段（１１）と、前記通信ネ

ットワークを流通する伝送情報の中から前記取得した条件情報に対応する通信システム又は通信システムグループ宛の伝送情報を捕獲する伝送情報捕獲手段（１２）と、捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する伝送情報選別手段（１３，１４，１５）と、前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す通知手段（１６）とを具備し、第２伝送情報を不正アクセスの蓋然性がある伝送情報として扱う構成。

【００１４】本発明は、また、上記のアクセス種別を判定する方法を汎用のコンピュータで実施する上で好適となる記録媒体を提供する。この記録媒体は、外部から行われるアクセスを正常アクセスとして受容するための伝送情報の特徴条件を定めた条件情報を管理対象となる通信システム又は通信システムグループ毎に更新自在に登録してなる条件情報登録手段と、各通信システム又は通信システムグループに対するアクセス条件の変更を行う条件変更手段とを有する通信ネットワークに接続される通信機能付きコンピュータに下記の処理を実行させるためのプログラムコードが記録された、コンピュータ読み取り可能な記録媒体である。

（１）前記条件情報登録手段から最新の前記条件情報を取得する処理、（２）前記通信ネットワークを流通する伝送情報の中から前記取得した条件情報に対応する通信システム又は通信システムグループ宛の伝送情報を捕獲する処理、（３）捕獲した伝送情報の中から前記取得した条件情報に適合する第１伝送情報と適合しない第２伝送情報とを選別する処理、（４）前記第２伝送情報が選別されたときに当該第２伝送情報に基づくアクセスを排除するためのアクセス条件の変更を前記条件変更手段に促す処理。

【００１５】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図１は、本発明が適用されるネットワークシステムの全体構成図である。このネットワークシステムには、インターネットα、ISDN及び電話網の公衆通信網β、内部ネットワークγが相互通信可能な形態で接続されている。内部ネットワークγには、管理対象となる通信システム又は通信システムグループ（ＬＡＮ等によってグループ化された通信システム群：以下、この実施形態では、「サイト」と称する）が接続されている。Ｔ１は、攻撃者が操作する端末すなわち不正アクセス発信源である。内部ネットワークγには、通常、その前段にファイヤーウォール等のセキュリティ機構が設けられている。

【００１６】ネットワークシステムには、さらに、複数の不正アクセス検知システム１０と、管理サーバ２０と、認証局３０とが接続されている。管理サーバ２０は、サイトのアクセス管理を行うものであり、不正アクセス検知システム１０は、管理サーバ２０によるアクセス管理の補助処理を行うものである。認証局３０は、求めに応じて、認証された電子証明書を発行するものである。この電子証明書は、後述するアクセスポリシーをやり取りして良い相手かどうかの認証を利用される。

【００１７】＜不正アクセス検知システムの構成＞不正アクセス検知システム１０は、プロトコルの仕様やサイト毎のアクセスポリシーに基づく正常アクセスのための条件情報と実際のアクセス内容とを比較していくことによって、正常アクセスではない、不正アクセスの蓋然性があるものを検知する。まず、この不正アクセス検知システム１０の構成について説明する。

【００１８】不正アクセス検知システム１０は、通信機能付きのコンピュータによって実現されるもので、その構成は図２に示されるとおりである。すなわち、プロトコル仕様データベースＤＢ１１、アクセスポリシーデータベースＤＢ１２、アラーム通知先データベースＤＢ１３、ネットワークインタフェースＩＮＴ１のほか、所定のプログラムコードを読み取って実行することにより形成されるアクセスポリシー取得モジュール１１と、パケット捕獲モジュール１２と、パケット選別モジュール１３と、プロトコル仕様違反検知モジュール１４と、アクセスポリシー違反検知モジュール１５と、通知モジュール１６と、これらのモジュールを統括的に制御する（補完処理を含む）主制御部ＣＯＮ１を具備するものである。上記のプログラムコードは、通常は、図示しない上記コンピュータの外部記録装置（ハードディスク等）に記録され、当該コンピュータのＣＰＵが適宜読み出して実行されるようになっているが、コンピュータ読み取り可能な可搬性の記録媒体に記録される形態や、プログラムサーバを介して上記外部記録装置に記録されるものであっても良い。

【００１９】ネットワークインタフェース１４は、管理サーバ２０との間の通信を制御したり、ネットワークシステムを流通する伝送情報、ここではパケットを取得する機能を有するものである。このネットワークインタフェース１４には、自己宛のMAC（Media Access Control）アドレスを持つパケットのみを捕獲するモードと、自己宛のＭＡＣアドレス以外の宛先を持つパケットも含めてネットワークシステムを流通するすべてのパケットを取得するモードの二つが用意されている。この実施形態では、後者のモードを利用する。

【００２０】アクセスポリシー取得モジュール１１は、管理サーバ２０からアクセスポリシーを取得するものである。具体的には、ＦＴＰ（File Transfer Protocol）プロトコル等によるファイル転送機能を利用して管理サーバ２０から管理対象となるサイトのアクセスポリシーをネットワーク経由で取得し、これをアクセスポリシーデータベースＤＢ１２に保持しておく。なお、管理サー

バ２０上のアクセスポリシーが変更された場合は、管理サーバ２０から新しいアクセスポリシーが送付されるようになっている。

【００２１】パケット捕獲モジュール１２は、ネットワークシステムを流通するパケットを捕獲（キャプチャリング）するものである。パケット選別モジュール１３は、管理対象となるサイトへのパケットを選別（パケットフィルタリング）するものである。具体的には、管理対象となるサイトのＩＰアドレスを登録しておき、そのＩＰアドレスを宛先ＩＰアドレスとして持つパケットのみを、捕獲されたパケットの中から選別する。

【００２２】プロトコル仕様違反検知モジュール１４は、プロトコル仕様に違反しているアクセスかどうかを予め登録されているプロトコル（IP、TCP、UDP、ICMP、HTTP、FTP、SMTP、DNS、TELNET等）毎に判定するものである。具体的には、パケット選別モジュール１３で選別されたパケットに対し、そのパケットで使用されている各プロトコルが仕様どおりに正しく使用されているかどうか、各プロトコルのヘッダの長さ、フィールドの構造、各フィールドの値、データの長さ、データの内容等が仕様で規定されている範囲であるか、各フィールドの値に矛盾がないかどうかをプロトコル毎に判定する。正しく使用されていないアクセスは、不正アクセスの蓋然性があると判定する。このプロトコル仕様判定は、プロトコル層別に行われ、まず、はじめにIPヘッダ、そして、トランスポート層ヘッダ（TCP、UDP、ICMP）、最後にアプリケーション層（HTTP、SMTP、DNS等）の内容が判定対象となる。

【００２３】アクセスポリシー違反検知モジュール１５は、サイトのアクセスポリシーに違反しているアクセスを検知するものである。ここでは、アクセスポリシーの一例として、アクセスポリシーデータベースＤＢ１２に保持されている、許可する送信元アドレス、宛先アドレス、利用プロトコル（ポート番号）の組み合わせと一致するパケットを選別する。この選別は、パケットのIPヘッダの送信元アドレス、宛先アドレス、プロトコルの各フィールドを調べることによって行う。不一致であった場合は、不正アクセスの蓋然性があると判定する。一致した場合には、引き続き、そのアクセスのアプリケーション層プロトコルの内容に含まれるサイト特有のパラメータ、例えばHTTPの場合はURL、SMTPの場合はコマンド名や電子メールアドレス等やデータの長さ等がアクセスポリシーによって許可されている内容であるかどうかをプロトコル毎にチェックする。許可されていないパラメータをもつアクセスについては、不正アクセスの蓋然性があると判定する。

【００２４】通知モジュール１６は、不正アクセスの蓋然性があると判定されたときに、その旨を表示したり、関係者に通知したりするものである。具体的には、対象となるアクセスがプロコトルの仕様に違反している場合、またはアクセスポリシーに違反している場合に、画面に警告分やアイコンとして表示したり、管理者宛にメールを送信したり、管理者のページャ（ポケベル）や携帯電話に通知したりする。アラーム通知先データベースＤＢ１３には、この通知の際に取るべきアクション（メールの発信、ポケベルの発信、画面上への表示等）とその通知先（メールの宛先、ポケベルの番号等）が予め登録されている。

【００２５】＜管理システムの構成＞次に、管理サーバ２０の構成について説明する。管理サーバ２０もまた、通信機能付きのコンピュータによって実現されるもので、その要部構成は図３に示されるとおりである。すなわち、サーバとしての本来の機能のほか、ネットワーク構成情報データベースＤＢ２１、登録情報データベースＤＢ２２、アクセス条件データベースＤＢ２３及びネットワークインタフェースＩＮＴ２のほか、所定のプログラムコードを読み取って実行することにより形成される登録情報管理モジュール２１と、アクション管理モジュール２２と、これらのモジュールの機能を統括的に制御する（補完処理を含む）主制御部ＣＯＮ２を具備する。プログラムコードは、通常は、図示しない上記コンピュータの外部記録装置（ハードディスク等）に記録され、当該コンピュータのＣＰＵが適宜読み出して実行されるようになっているが、コンピュータ読み取り可能な可搬性の記録媒体に記録される形態や、プログラムサーバを介して上記外部記録装置に記録されるものであっても良い。

【００２６】ネットワーク構成情報データベースＤＢ２１は、管理対象となるネットワークシステム全体の構成情報を蓄積するものである。この構成情報は、アクセスポリシーやプロトコル仕様（以下、「アクセスポリシー等」）を配布したり、アクション条件を変更する際に参照される。

【００２７】ネットワークインタフェースＩＮＴ２は、主として、不正アクセス検知１０、認証局３０及び内部ネットワークァの前段に設けられるファイアウォール等との通信制御を行う。登録情報管理モジュール２１は、新規ホストからのアクセスポリシーやプロトコル仕様、あるいは、新規不正アクセス検知システム１０からのアドレスと電子証明書（必要に応じて）の登録を受け付け、これらを登録情報データベース２１に保持するとともに、求めに応じてあるいは自律的に、アクセスポリシー等を不正アクセス検知システム１０に配布するものである。アクセスポリシー等が変更された場合には、変更された内容を配布する。配布は、ＦＴＰ（File Transfer Protocol）プロトコル等によるファイル転送機能を利用し、ネットワーク経由で行う。その際、アクセスポリシー等が攻撃者に取得されないようにするため、これを共通鍵暗号方式等によって暗号化し、認証された電子証明書を添付する。アクセスポリシー等を配布するタイミ

ングは、不正アクセス検知システム１０が新たに設置された場合またはアクセスポリシー等が管理者によって変更された場合である。

【００２８】アクション管理モジュール２２は、不正アクセス検知システム１０から不正アクセスの蓋然性があるアクセスを検知した旨の通知を受けた場合に、後続のアクションをとるための条件（管理者へのアラームの送信方法等）や対象となるサイトへのアクセス条件（アクション条件）を変更するものである。サイトへのアクセス条件としては、例えば、ファイアーウォールの設定変更、コネクションの切断、発信源の追跡指示等が挙げられる。

【００２９】より具体的には、不正アクセス検知システム１０からの通知内容と、そのアクセス内容のサマリ（宛先IPアドレス、利用プロトコル、送信元IPアドレス等）とをアクション条件データベースＤＢ２３に保持しておき、必要に応じて、管理者が現在のアクション条件をブラウザ等のインタフェースから変更できるようにする。変更された後は、同様の通知結果（プロトコル仕様判定の結果とアクセスポリシー判定の結果を並べたもの）となる不正アクセスについては、その変更後のアクション条件が適用される。不正アクセス検知システム１０からの通知結果が同様となるアクセスについては、たとえ攻撃に使用するプログラム等の手法が異なっていても同様の結果を引き起こすものと予想されるため、未知の不正アクセスでも、既知の不正アクセスのチェック結果パターンと同じであれば、その被害の度合を予測することができ、適切なアクションを行うことが可能となる。

【００３０】＜アクセスの種別判定方法＞次に、上記の不正アクセス検知システム１０及び管理サーバ２０を用いてアクセスの種別を判定する方法の実施形態を説明する。本実施形態の方法では、不正アクセス検知システム１０が図１のネットワークシステムにおけるパケットの流通形態のセンサとして機能するので、不正アクセス検知システム１０における処理手順（主制御部ＣＯＮ１の統括的な制御に基づく各種モジュールの実行による処理）を中心に説明する。図４はその全体処理手順図、図５～図９は具体的な内容説明図である。

【００３１】まず、本実施形態において不正アクセスの蓋然性が高いとして検知されるアクセスの概念を図５の例により明らかにする。図５は、外部にその存在を知らしめていない内部ホストＭ１、SMTPアクセスのみを受容するメールサーバＭ２、URLを公開しているWWWサーバＭ３をそれぞれ管理対象サイトとする場合の例である。この場合、内部ホストＭ１へのアクセスＬ１はすべて検知される。メールサーバＭ２へのアクセスＬ２については、正常なSMTPアクセスは検知されないが、SMTPアクセス以外、許可していないSMTPコマンドによるアクセス、正しくない形式のメールはすべて検知される。WWWサーバＭ３のアクセスＬ３については、公開しているURLによる正常なWWWアクセスは検知されないが、それ以外のアクセスは、すべて検知される。

【００３２】図４を参照し、上記のようなアクセスの種別を判定できるようにするため、不正アクセス検知システム１０は、管理サーバ２０から管理対象となるサイトのアクセスポリシー及びプロトコル仕様のデータをダウンロードして保持しておく（ステップＳ１０１）。既に保持してあるデータが変更された場合はそれらを更新する。図６は、保持されているデータの内容例を示した図である。

【００３３】図６の上段は、「a.b.c.d」という「宛先アドレス」を持つサイトに対するインターネットα上の「すべて」の「送信元アドレス」を持つ端末からの「http／tcp」プロトコル仕様によるアクセスについては、これを正常アクセスとして扱うべきことを意味している。同様に、「a.b.c.e」という「宛先アドレス」を持つ端末に対するインターネットα上の「すべて」の「送信元アドレス」を持つ端末からの「smtp／tcp」プロトコル仕様によるアクセスも正常アクセスとして扱われる。「プロトコル特有の条件」もプロトコル仕様の範囲であり、ここでは許可するプロトコル別の条件を指定する。例えばWWW（HTTP）の場合は、閲覧を許可するディレクトリ／ファイルとURLの最大長を指定する。但し、これらのプロトコルとそれに対応する指定項目は、予め管理サーバ２０に登録しておく必要がある。図６の例では、WWWサービス（プロトコルがHTTPの場合）では、「公開するファイル」と使用するURLの「最大文字長」を指定することができ、ルートディレクトリの下の「／Index．html」ファイル、「／whatsnew／＊」、「／products／＊」、「／profile／＊」（＊は任意の文字列を示す。）のディレクトリ配下のすべてのファイルへのアクセスを許可することを示している。その他、「プロトコル特有の条件」では、社内で「使用するメールアドレス」や使用を「許可するコマンド」等を指定させることもできる。

【００３４】図４に戻り、アクセスポリシー等をダウンロードした不正アクセス検知システム１０は、ネットワークシステム上を流通するパケットを常時監視し、管理対象となるサイト宛のパケットがあった場合はそれを捕獲する（ステップＳ１０２）。これは、流通するパケットのヘッダ情報等を参照することによって行う。その後、捕獲したパケットに対して、プロトコル仕様チェック及びアクセスポリシーチェックを行う（ステップＳ１０３）。

【００３５】図７は、プロトコル仕様チェックの概念の一例を示した図である。プロトコル仕様チェックは、プロトコル仕様データベースＤＢ１１に保持されているIPヘッダ、トランスポート層ヘッダ、アプリケーション層というようにプロトコル層別の一致性をみることで行

う。図７には、HTTPプロトコル仕様の場合の例が示されている。HTTPプロトコル仕様のもとでは、IPヘッダ、TCPヘッダ、HTTPヘッダ、HTTPデータの順にチェックされる。チェック内容は、パケットにおけるIPヘッダの各フィールドの値が正しい範囲に収まっているかどうか、IPヘッダのIPパケット全体長フィールドの値とIPヘッダ長フィールドの値に矛盾がないかどうか（IPパケット全体長はヘッダ長よりも長くなくてはならない。）等である。否定的であった場合は、違反するパケットとする。TCPヘッダもIPヘッダと同様の内容となる。その後、HTTPヘッダの各フィールドのフォーマットが仕様通りに記述されているか、HTTPデータのフォーマットが仕様通りに記述されているかどうかのチェックが続く。HTTPプロトコルの仕様は、標準規格であるRFC1945やRFC2068に記述されているので、これを参考にすることができる。例えば、HTTPのリクエストのデータ部には、以下の形式の内容が含まれることになっている。なお、実際には“GET”以外にも“POST”等があるが、ここでは省略する。

GET“Request－URL”HTTP／1.1（バージョン1.1の場合）

GET“Request－URL”HTTP／1.0（バージョン1.0の場合）

GET“Request－URL”

このとき、“Request－URL”というパラメータには、サーバへ要求するURLが挿入される。この段階では、このようなサイト特有の内容まではチェックせずに、その他の部分が仕様に合っているかどうかをチェックする。仕様にあっていない場合（“HTTP／1.0”や“HTTP／1.1”以外の文字列が存在している等）、この時点で、不正アクセスの蓋然性があると判定する。

【００３６】一方、アクセスポリシーチェックでは、パケット中の「宛先アドレス／送信元アドレス／利用プロトコル（＝TCP及びUDPのポートの番号）」の内容を、アクセスポリシーデータベースＤＢ１２に登録されている、当該サイトで許可するアクセスポリシーの内容と比較し、一致していなければ違反するパケットであると判定する。先ほどの仕様のチェックでは行わなかった”Request-URL”の内容のチェックは、ここでアクセスポリシーチェックとして行う。なお、プロトコル仕様チェックとアクセスポリシーチェックでは、少しでも不一致があれば違反するパケットと判定するが、特定部分の不一致については、これを不問とする扱いも可能である。なお、プロトコル仕様チェックとアクセスポリシーチェックについては、両方を判定するのが好ましいが、必要に応じて、いずれか一方のみを判定するようにしても良い。

【００３７】以上の各チェックの結果、違反しないパケットであれば、正常アクセスであることを意味するので、それが流通することに対して何らの処理を行わない（ステップＳ１０４：No）。一方、違反するパケットは、実際に不正アクセスによるものかどうかを問わず、不正アクセスの蓋然性があると判定する（ステップＳ１０４：Yes）。このチェック結果は、図示しないジャーナル管理機構に、チェック履歴として記録しておく。このチェック履歴の一例を示したのが図９である。図９（ａ）は、プロトコル仕様チェックの結果、同（ｂ）は、アクセスポリシーチェックの結果の履歴である。

【００３８】違反したパケットであった場合は、当該パケットに関する情報（送信元アドレス等）を特定するとともに（ステップＳ１０５）、アラーム通知先データデースＤＢ１３を参照して、通知手段及び通知内容を特定し（ステップＳ１０６）、通知処理を実行する（ステップＳ１０７）。

【００３９】アラーム通知先データデースＤＢ１３には、図８に示される内容例が登録されているので、該当する「通知先」に、該当する「通知内容」で不正アクセスの蓋然性があるパケットを検知した旨を通知する。これにより、通知された側では、該当するアクセスに対する注意が喚起されるので、不正アクセス回避のためのアクションをとることができるようになる。通知先が管理サーバ２０である場合には、アクション管理モジュール２２によって、以後のアクションをアクション条件データベースＤＢ２３の登録内容に従って自動実行させることができる。

【００４０】このように、本実施形態の方法によれば、未知の手法を含む広範囲の不正アクセスを検知できるようになる利点がある。また、従来のように統計的方式を採用して不正アクセスかどうかを判定するものではないので、その基準が攻撃者に操作されることもなく、安定的な運用が可能になる。さらに、ユーザ毎のプロファイルを扱わないので、不特定多数のユーザがアクセスする通信ネットワーク環境にも柔軟に対応することができる。さらに、アクセス中の実際のパケットを用いて不正アクセスの蓋然性の有無をリアルタイムで検知しているため、その後の対策、例えば発信源の追跡やファイアーウォールの条件変更による防御等が迅速になる利点もある。

【００４１】なお、本実施形態では、直接的には触れていないが、プロトコル仕様やアクセスポリシーのほか、上述のプロトコルポリシーや、単位時間あたりのアクセスの回数がアクセスポリシーに記述されているアクセスの許容頻度以内であるかどうかも、必要に応じて考慮するようにしても良い。

【００４２】

【発明の効果】以上の説明から明らかなように、本発明の方法によれば、未知の手法を含めた広範囲のアクセス種別を判定することができ、且つ判定の基準を攻撃者に操作されることがないという、特有の効果を奏する。また、本発明のシステムによれば、通信ネットワーク経由で行われる広範囲な不正アクセスを検知し、それを回避

するためのアクションを迅速にとれるようになるという、効果を奏する。

【図面の簡単な説明】

【図１】本発明が適用されるネットワークシステムの全体構成図。

【図２】不正アクセス検知システムの機能構成図。

【図３】管理サーバの機能構成図。

【図４】不正アクセス検知システムの手順説明図。

【図５】本実施形態において違反とされるアクセスの概念を示した図。

【図６】アクセスポリシー及びプロトコル仕様の例を示した図。

【図７】プロトコル仕様チェックの概念を示した図。

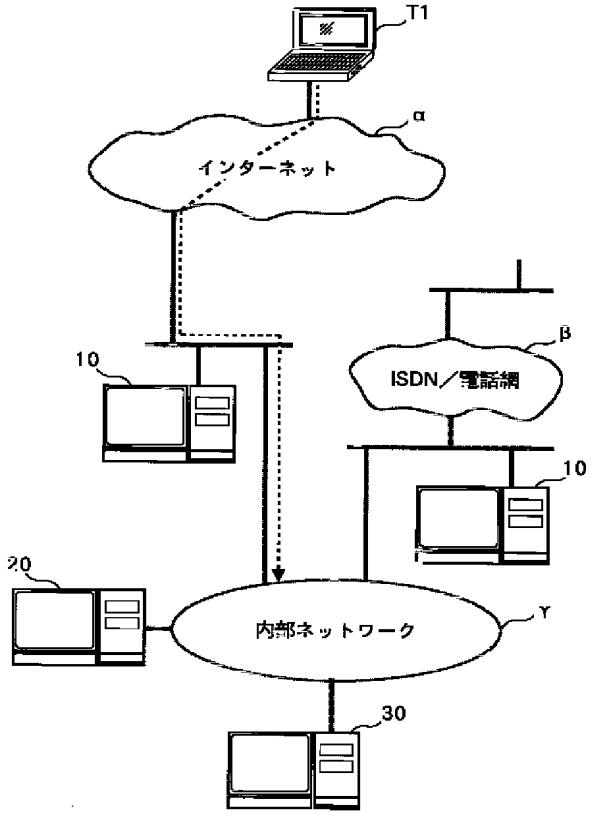
【図８】アラーム通知先データベースの内容例を示した図。

【図９】（ａ）はプロトコル仕様チェックの結果、（ｂ）はアクセスポリシーチェックの結果の一例を示した図。

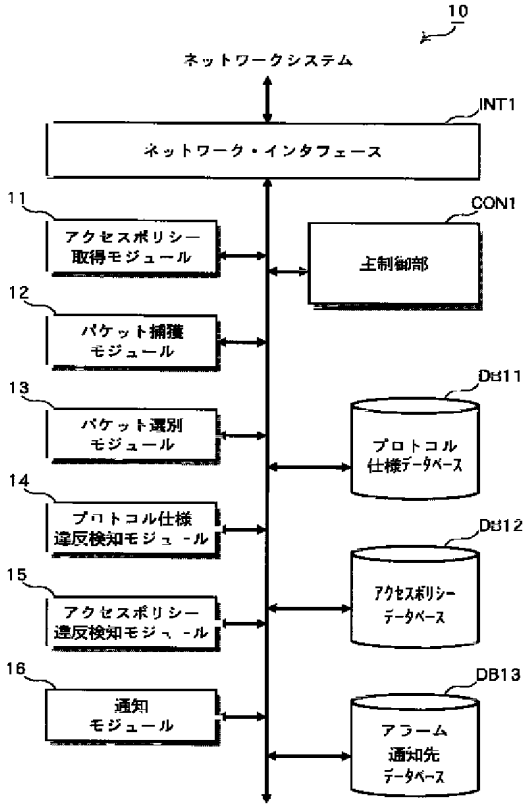
【符号の説明】

１０　不正アクセス検知システム
１１　アクセスポリシー取得モジュール
１２　パケット捕獲モジュール
１３　パケット選別モジュール
１４　プロトコル仕様違反検知モジュール
１５　アクセスポリシー違反検知モジュール
１６　通知モジュール
２０　管理サーバ
２１　登録情報管理モジュール
２２　アクション管理モジュール
ＤＢ１１　プロトコル仕様データベース
ＤＢ１２　アクセスポリシーデータベース
ＤＢ１３　アラーム通知先データベース
ＤＢ２１　ネットワーク構成情報データベース
ＤＢ２２　登録情報データベース
ＤＢ２３　アクション条件データベース
ＩＮＴ１，ＩＮＴ２　ネットワークインタフェース
ＣＯＮ１，ＣＯＮ２　主制御部
３０　認証局
Ｔ１　不正アクセス発信源
α　インターネット
β　ISDN／電話網
γ　内部ネットワーク

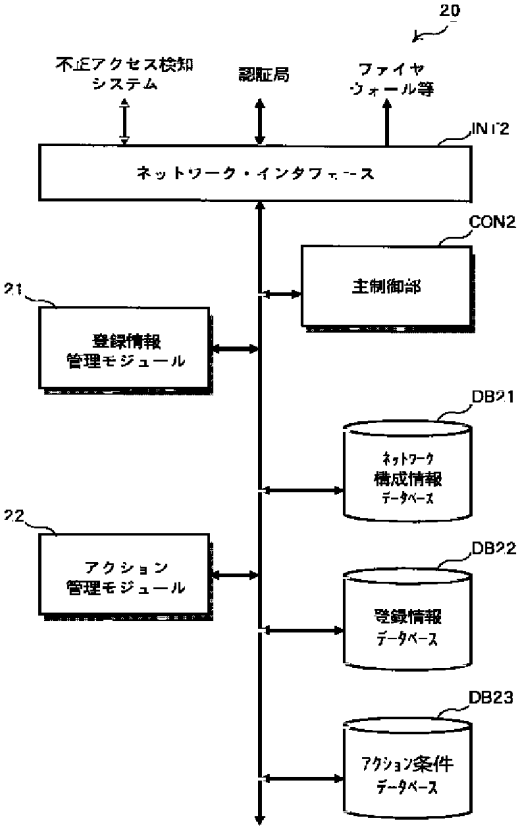
【図１】



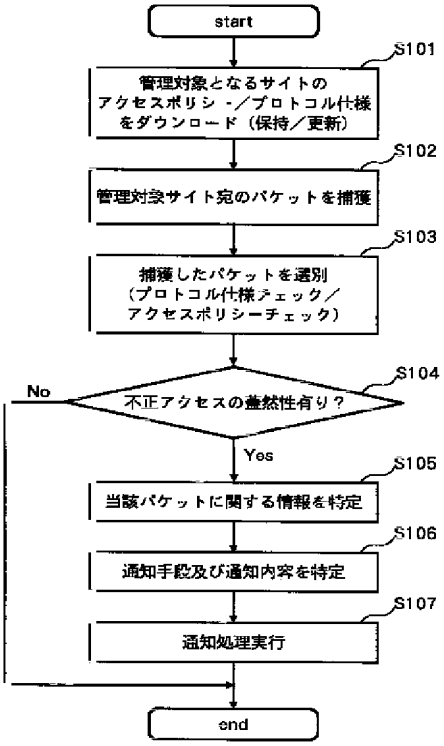
【図２】



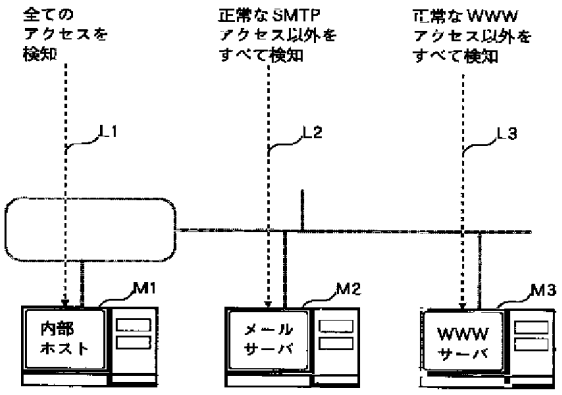
【図3】



【図4】



【図5】



【図6】

送信元アドレス	宛先アドレス	プロトコル	ユーザ名	プロトコル特有の条件
すべて	a.b.c.d	http/tcp	ANY	公開するファイル /index.html /whatsnew/* /profile/* ・・・・・・・・・
すべて	a.d.c.e	smtp/tcp	ANY	使用するメールアドレス ****@a.co.jp *****@b.co.jp 許可するコマンド VRFY、EXPN

【図7】

IPヘッダ	TCPヘッダ	HTTPヘッダ	HTTPデータ

【図８】

通知手段	通知先	通知内容	使用
電子ﾒｰﾙ	postmaster@a.co.jp	不正アクセスが発生しました 送信先： 宛先： ﾌﾟﾛﾄｺﾙ：	○
ﾎﾟｹﾍﾞﾙ	03－1234－5678	不正アクセスが発生しました 送信先： 宛先： ﾌﾟﾛﾄｺﾙ：	×
ｺﾝｿｰﾙ		不正アクセスが発生しました 送信先： 宛先： ﾌﾟﾛﾄｺﾙ：	○
…	……	……	

【図９】

(a)

プロトコル仕様違反検知モジュール	チェック項目	チェック結果
ＩＰ	IPヘッダ長	正常
	IP全体長	正常
	フラグメント	正常
TCP	TCPヘッダ長	正常
ＨＴＴＰ	リクエスト形式	違反

(b)

アクセスポリシー違反検知モジュール	チェック項目	チェック結果
ＩＰ	宛先アドレス	正常
	送信元アドレス	正常
TCP	宛先ポート	正常
	送信元ポート	正常
ＨＴＴＰ	URL内容	違反

フロントページの続き

(72)発明者　小久保　勝敏
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　松田　栄之
東京都江東区豊洲三丁目３番３号　株式会社エヌ・ティ・ティ・データ内

Ｆターム(参考)　5B089 GA11 GA21 GB02 HA03 HA06 HA10 JA22 JA31 JB22 KA17 KB04 KB06 KB13
5K030 GA15 HB16 HB18 HC01 KA04 KA13 LA08 LB02 LD19 LD20
9A001 CC06 JJ14 JJ25 LL03